

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Criminal No. 18-067 (WMW)

UNITED STATES OF AMERICA,)
)
Plaintiff,)
) GOVERNMENT'S POSITION
v.) WITH RESPECT TO SENTENCING
)
TERRY J. ALBURY,)
)
Defendant.)

The United States Department of Justice, National Security Division, Counterintelligence and Export Control Section, and the Office of the United States Attorney for the Eastern District of Virginia (collectively, the “Government”), hereby submit the Government’s position with respect to sentencing of Terry J. Albury (“Albury” or “defendant”).

I. THE CASE AGAINST THE DEFENDANT

As early as February 2016, the defendant began manipulating classified information on Federal Bureau of Investigation (“FBI”) computer systems. This course of conduct continued until a search warrant was executed at the defendant’s home on August 29, 2017. The FBI’s investigation has shown that the defendant’s manipulation of classified information—which, to avoid detection, included photographing it and removing it from secure space on digital media, or cutting-and-pasting it into separate documents for printing—was part of a greater scheme to retain classified national defense information in unauthorized locations and to provide it to the media. In all, the defendant stole government information from more than 70 documents, of which approximately 50 were classified. Doing so was not only against the law, but a betrayal of the oath that the defendant took to protect classified information. As defendant well knew, his actions could result in serious harm to our national security.

The defendant's sentence of imprisonment must reflect the length of time during which the defendant's criminal activity took place, the number of classified documents involved, the defendant's exploitation of his position as a trusted insider, and the various means employed by the defendant to avoid detection. The Government also acknowledges, however, that the defendant accepted responsibility and agreed to plead guilty pre-indictment, saving the government resources as well as the need to risk disclosure of additional classified information in order to prove its case at trial. Accordingly, a sentence at the midpoint of the sentencing guideline range of 46-57 months is appropriate.

A. The Charges of Conviction

On April 17, 2018, the defendant pleaded guilty to a two-count Information charging him with unlawful transmission and unlawful retention of national defense information, both in violation of 18 U.S.C. § 793(e). Both offenses carry a statutory maximum sentence of ten years' imprisonment, a three-year term of supervised release, a \$250,000 fine, and a \$100 special assessment.

B. The Defendant's Offense and Relevant Conduct

1. The Factual Basis in the Plea Agreement

As agreed to, among other facts, by the parties in the plea agreement:

Beginning from on or about February 2016, and continuing through on or about August 29, 2017, the defendant unlawfully retained and transmitted classified national defense information, including the documents specified in the Information.

The defendant had secretly taken FBI information and information belonging to other government agencies for approximately 18 months, using a variety of means to exfiltrate the information to avoid detection, including: cutting-and-pasting information from documents into other programs, and printing those materials so as to not leave a record of having printed a particular document; and accessing documents on his classified

FBI computer system and taking photographs of documents on his classified computer screen.

The defendant transmitted sensitive and classified documents containing National Defense Information to a person not entitled to receive it; to wit, Reporter A. The defendant further retained classified documents containing National Defense Information on a number of digital storage media devices and in a number of locations at his residence.

The defendant received training regarding classified information, including the definitions of classified information, the levels of classification, as well as the proper handling, marking, transportation, and storage of classified materials. The defendant received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage requirements.

The defendant was never authorized to retain these documents at his residence or to transmit them to any person not entitled to receive them, and the defendant knew that he was not so authorized.

2. *Additional Facts in the PSR*

As described below, the PSR provides additional relevant information about the offense conduct (PSR ¶¶ 6-13), and notes other relevant conduct, including the means defendant employed to hide his conduct (PSR ¶¶ 11-12), the volume of materials, and the various agencies to which the stolen information belongs (PSR ¶ 13). The PSR provides a sufficient record of the defendant, his background, and much of his conduct. The Government is attaching hereto an unclassified declaration of E.W. Priestap, Assistant Director of the FBI's Counterintelligence Division (Attachment 1), which explains why the materials were classified and the harms that could result from the defendant's actions.

The volume of materials involved is substantial. The search of Albury's residence uncovered a micro-SD card that contained copies of more than 50 documents, 35 of which contained classified information from multiple government agencies. *See* Priestap Decl. ¶ 16. The SD card was in an envelope that had a post-it note with the telephone number of a reporter, identified as Reporter A in the Plea Agreement, affixed to it. (PSR ¶ 13).

3. Additional Facts Agreed to by the Parties

Certain additional uncontested facts that do not appear in the PSR are described below.¹

On March 24, 2017, the defendant installed a new operating system on his laptop. This installation wiped most, but not all, of the data that was previously stored on that system. On the defendant's laptop the FBI discovered a foreign-based email account, peaceispatriotic@tutanota.com. Tutanota is a German email provider that offers end-to-end encryption of email. The defendant searched FBI systems for the name of the foreign email provider on March 7, 2017.

Based on the FBI's review of 120 days of login times, the defendant usually arrived in his workspace between 7:40 and 8:10 am. Specifically, his median login time was 7:51 am, with about 50% of all logins occurring between 7:40 and 8:10 am. On April 7, 2017, he arrived in his workspace at 6:11 am. On May 4, 2017, he arrived at 7:10 am. On May 9, 2017, he arrived at 7:06 am. On June 16, 2017, he arrived at 7:45 am. On August 23, 2017, he arrived at 7:08 am. On August 24, 2017, he arrived at 6:31 am. On June 16, August 23, and August 24, video surveillance captured the defendant photographing his classified computer screen. On April 7, May 4, and May 9, the defendant accessed classified documents, photographs of which were later recovered on the storage device seized from his home.

On or about April 12, 2017, the defendant installed Adobe Acrobat software and the Readdle PDF Expert application, both of which provide the capability to assemble .pdf files from photographic images. The account registration for the software applications used the Tutanota email account mentioned above. On April 13, 2017, the defendant created two .pdf files. The external storage device recovered from the defendant's home contained, in addition to individual

¹ Defense counsel indicted no dispute with these facts, which obviated the need for the government to move for an evidentiary hearing.

photographic images, two .pdf files. One file contains 22 separate documents and the other contains two FBI policy guides. Both of these .pdf files were compiled from the photographs the defendant took of 24 documents (13 of which were classified), on April 7, 2017. The external storage device contained these two .pdf files along with photographic images of the materials the defendant photographed on June 16, August 23, and August 24, 2017.

Finally, on June 10, 2017, an install file for Tor Browser Version 7.0 was created on the defendant's laptop.²

C. The Pertinent Guideline Calculations

The parties agree on the base offense level but disagree as to the enhancement for abuse of a position of trust.

Base Offense Level, § 2M3.3	24
Specific Offense Characteristics, § 3B1.3	+2
Acceptance of Responsibility, § 3E1.1(a)	<u>-3</u>
Total guideline range	23 (46-57 months)
Total guideline range without enhancement	21 (37-46 months)

The parties agree that no other specific offense characteristics or Chapter 3 adjustments should apply and that the defendant's criminal history category would be I. Notwithstanding the defendant's attempts to minimize his criminal conduct in his statement to probation (*e.g.*, PSR ¶ 18 at p.6), the defendant will receive in conjunction with his guilty plea a two-level reduction pursuant to § 3E1.1(a), and the Government further hereby moves for the additional one-point reduction for entry of a timely plea.

² Tor is free software that allows private internet browsing and enables anonymous communication.

The Standard for Abuse of a Position of Trust

Section 3B1.3 of the sentencing guidelines provides that a two-level enhancement should apply where the defendant “abused a position of public or private trust . . . in a manner that significantly facilitated the commission or concealment of the offense.” U.S.S.G. § 3B1.3; *see United States v. Erhart*, 415 F.3d 965, 972 (8th Cir. 2005); *United States v. Jankowski*, 194 F.3d 878, 884 (8th Cir. 1999) (citing U.S. Sentencing Guidelines Manual § 3B1.3 commentary (n.1)). To apply this standard, the Eighth Circuit inquires as to ““whether trust is inherent to the nature of the position.”” *Erhart*, 415 F.3d at 972 (quoting *United States v. Brelsford*, 982 F.2d 269, 272 (8th Cir. 1992)). That is clearly the case here, where the conduct involved an agent of the FBI who possessed a security clearance. *See United States v. Shyllon*, 10 F.3d 1, 5-6 (D.C. Cir. 1993) (recognizing that law enforcement officials occupy a position of trust and the enhancement applies if the position “provides the freedom to commit a difficult-to-detect wrong”) (citing *United States v. Queen*, 4 F.3d 925, 928-29 (10th Cir. 1993)).

The evidence fully supports this finding. Albury’s specialized access to some of the nation’s most closely guarded secrets by virtue of his security clearances and employment at the FBI vastly enhanced his ability to commit the crimes and have them go undetected. The defense suggests, however, that the enhancement is inappropriate because it is somehow already incorporated into the base offense level for the offense under § 2M3.3. Appendix to the PSR (PSR Appx.) at A1. The defense cites no authority for that argument. Indeed, the relevant legal authority is to the contrary. *United States v. Ford*, 288 F. App’x 54, 60-61 (4th Cir. 2008) (finding no error in district court determination that defendant, who held a Top Secret clearance at the NSA, warranted an enhancement “because his abuse of his position of public trust contributed significantly to his commission of the offense”); *cf. United States v. Pitts*, 973 F.

Supp. 576, 584 (E.D. Va. 1997) (increasing abuse of position enhancement by one additional level for former FBI agent convicted of violating 18 U.S.C. § 794 who “held a special position of awesome responsibility and trust [and] was supposed to safeguard this nation from foreign espionage activity” but who “[i]nstead . . . betrayed his country by engaging in the very activity that he was sworn to protect the nation against”), *aff’d*, 176 F.3d 239, 245 (4th Cir. 1999) (affirming district court’s enhancement where “abuse of trust was extraordinary”).

The defendant’s articulated position is also at odds with the plain language of the statute, which authorizes punishment for “[w]hoever having unauthorized possession of . . . [materials] related to the national defense . . . willfully communicates . . . or willfully retains the [national defense materials]. As recognized by Probation, subsections (d) and (e) of 793 cover a range of individuals of different status and access to classified information in the disclosure of national defense information to other individuals not authorized to receive it. PSR Appx. at A.2; *see United States v. Morison*, 844 F.2d 1057, 1063-1071 (4th Cir. 1988).

The statute does not require that the classified information be entrusted in any way to the defendant. The mere fact that the defendant was an employee or officer of the victim does not mean that abuse of a position of trust is an element of the offense, nor does it mean that the application of U.S.S.G. § 3B1.3 is inappropriate. For example, a clerk, janitor, or other employee not occupying a position of trust could obtain and unlawfully communicate national defense information in violation of 18 U.S.C. § 793(e). Section 793(e) does not contain any element, therefore, that would preclude the application of U.S.S.G. § 3B1.3 in this case. Rather, it was the defendant’s particular position of trust that gave him access to FBI’s classified computer systems containing sensitive information from a number of different federal agencies. This access, coupled with the relative autonomy he enjoyed in his job, enabled the defendant to manipulate,

print, and photograph sensitive documents from the classified system, surreptitiously remove them from FBI facilities, and, ultimately, transmit them to the media. His position of trust, therefore, “significantly facilitated the commission or concealment of the offense.” U.S.S.G. § 3B1.3; *see Shyllon*, 10 F.3d at 5-6. This is also consistent with forms he signed relating to workplace searches, in which he acknowledged that “by granting me access to classified information, the United States Government is placing special confidence and trust in me.” *See Attachment 2.*

So too, as noted in the PSR, related statutes refer to the same set of guidelines. As with 793(e), the relevant statute here, 18 U.S.C. § 798(a) and 50 U.S.C. § 783(b) by their own terms do not require a position of trust for prosecution. PSR Appx. at A.3; *see United States v. Fondren* 1:09-cr-00263-CMH Dkt 137 (Feb 22, 2010 sentencing transcript at 27) (finding abuse of trust enhancement appropriate in prosecution for violation of 50 U.S.C. § 783). To amplify the point, a foreign agent who receives classified information would have engaged in criminal conduct under 50 U.S.C. 783(b), but would not be subject to an enhancement for abuse of a position of trust. This is also entirely consistent with the prosecution of foreign agents under the espionage statute, 18 U.S.C. § 794, who obviously do not occupy a position of trust vis-à-vis the United States. *E.g., United States v. Soussoudis*, (E.D. Va. 1:85-cr-00156-RLW) (Ghana national charged with variety of national security crimes); *United States v. Ogorodnikov*, (C.D. Cal. 2:84-cr-00972-RMT) (two Soviet emigres charged with espionage along with FBI agent Richard Miller); *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980) (Vietnamese citizen convicted of espionage along with U.S. citizen Ronald Humphry). The guideline for a violation of 18 U.S.C. § 794 – 2M3.1 – is structured in the same manner as the guideline for a violation of

§ 793, with one base offense level for Top Secret information and another for “other” information.

Indeed, all of the related guidelines for national security crimes premised on classified or national defense information – §§ 2M3.1, 2M3.2 and 2M3.3 – maintain the same structure whereby Top Secret information has a higher baseline score than other information, and the relevant guideline depends on the statute violated and accompanying level of criminal intent. *See* § 2M3.2 (Commentary; Statutory Provisions); *see also United States v. Chung*, 659 F.3d 815, 835 (9th Cir. 2011) (finding that § 2M3.2 the most appropriate sentencing guideline in connection with convictions involving unclassified information under 18 U.S.C. §§ 951 and 1831, and noting that “[c]onsidering that the conduct underlying Defendant's offense involved gathering national defense information [related to space and military vehicles], the district court did not err in choosing section 2M3.2 as the most analogous guideline applicable to the foreign agent conviction”). Nowhere, in all of the associated statutes and guidelines, is there an indication that only an individual occupying a position of trust can violate them. Thus, because all are applicable to violations by individuals who occupy positions of trust, and those who do not, the guidelines necessarily do not incorporate an enhancement for an abuse of a position of trust.

For these reasons, the PSR appropriately increased Albury’s offense level by two levels as required by § 3Bl.3.

II. THE PSR’s CALCULATIONS AND RECOMMENDATIONS

On July 26, 2018, the United States Probation Office disclosed to the parties and the Court the PSR in this case. The PSR calculates the defendant’s applicable guideline range at 46-57 months’ imprisonment, based on a total offense level of 23, criminal history category I, and a

statutory maximum sentence of 10 years' imprisonment. (PSR ¶¶ 75-78). The PSR also sets forth the statutory maximum periods of supervised release (3 years) and probation (5 years; although the defendant is ineligible for probation under the guidelines). (PSR ¶¶ 79-82).

The government has no objections to the PSR and agrees with the facts contained therein, with the addition of those facts outlined above. The government also agrees with the guideline calculations contained in the PSR and notes that they align with the calculations set forth by the government.

III. THE 18 U.S.C. § 3553(a) FACTORS SUPPORT THE GOVERNMENT'S PROPOSED SENTENCE

In *Gall v. United States*, 552 U.S. 38 (2007), the Supreme Court set forth the appropriate sentencing methodology: the district court calculates the advisory Guidelines range and, after hearing from the parties, considers the 18 U.S.C. § 3553(a) factors to determine an appropriate sentence. 552 U.S. at 49-50; *United States v. Ruvalcava-Perez*, 561 F.3d 883, 886 (8th Cir. 2009) (“In sentencing a defendant, the district court should first determine the appropriate Guidelines range, then evaluate whether a traditional departure is warranted, and finally decide whether or not to impose a guideline sentence after considering all the § 3553(a) sentencing factors.”).

The district court may not assume that the Guidelines range is reasonable, but instead “must make an individualized assessment based on the facts presented.” *Gall*, 552 U.S. at 50. If the court determines that a sentence outside of the Guidelines is called for, it “must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance.” *Id.* Section 3553(a) requires the Court to analyze a number of factors, including, “the nature and circumstances of the offense,” “the history and characteristics of the defendant,” “the need for the sentence to reflect the seriousness of the offense,” “the need for

deterrence,” “the need to protect the public from further crimes of the defendant,” and “the need to avoid unwarranted disparities.” 18 U.S.C. § 3553(a).

A. Nature and Circumstances of the Offense

The unauthorized retention and dissemination of classified national defense information is an extremely serious offense. That the defendant came into possession of these items by stealing them from secure FBI systems only heightens the egregious nature of his conduct. So too, defendant’s abuse of his position allowed the criminal endeavor to carry on for well over a year without detection. In short, the defendant stole information from more than 70 documents, of which approximately 50 were classified, *see* Priestap Decl. at ¶¶ 15-16, involving multiple government agencies, over an 18-month span.

Further, the criminal behavior at issue here does not represent the actions of one motivated by social conscience. Putting aside that defendant’s motive is irrelevant to the offenses, and that his behavior is directly contrary to his oath and the multiple non-disclosure agreements he signed, any proffered benign motive is also inconsistent with the facts. Here, the search of defendant’s home resulted in the recovery of more than 50 additional documents, 35 of which were marked classified at the Secret level. Given his manipulation of the materials, it is readily apparent that if the FBI had not disrupted the defendant’s conduct, the defendant would have continued to disclose our country’s secrets and likely damaged our national security.

Defendant claimed in his statement to Probation that the manner in which he possessed the materials at home “created the potential for the device to be provided to the journalist by someone else without [defendant’s] knowledge”—ignoring his previous behavior and imputing culpability to others when he himself transmitted classified information to Reporter A (PSR ¶ 18 at p.6). That contention requires a conscious disregard of the remaining facts and complete

suspension of disbelief. Defendant was not merely attempting to keep some library of classified information hidden at his home that risked inadvertent disclosure, and he carefully made no claim as to why he had those documents. Rather, defendant moved classified materials that he had taken from the FBI to his personal laptop and manipulated them into a different format (essentially laundering the information) using a program he downloaded using an anonymous email service. He then reloaded the materials onto a micro-SD card that was in an envelope to which was affixed the telephone number of Reporter A—the exact same Reporter to whom he previously disclosed information. To believe that somehow these particular documents were not intended for disclosure to the media defies belief.

The defense persists in this inconsistent argument, however, as it is the only way to attempt to minimize defendant's behavior in repeatedly providing without authorization classified national defense information to the media. The defense put out a statement the day of the defendant's guilty plea contending that the FBI "intimidated minority communities," and further that the defendant appreciated the support of those who "criticized the criminalization of disclosure of documents that chronicle and demonstrate government abuse." (PSR ¶ 17 at pp.4-5). The materials charged in the Information relate to terrorist threats and recruiting efforts, and the development of human sources.³ The other classified national defense information involved in this case similarly belies any assertion that the defendant was documenting "abuses" at the FBI. The materials gathered from defendant's home related to, among other things, counterintelligence priorities and information collected pursuant to the Foreign Intelligence Surveillance Act. These documents chronicle no "abuse" of any sort. Even apart from the

³ The Government does not believe this is necessary given the accompanying declaration from the FBI, but the Government can make the relevant documents available in a secure format for cleared personnel should the Court deem it necessary.

documents themselves, the defendant never availed himself of known opportunities to report any purported malfeasance. Nor did he seek out the Department of Justice's Office of Inspector General. Defendant's actions put us all at risk, and had those materials not been recovered in the search of Defendant's home, there could have been substantial additional risks to the FBI and other agencies.

As detailed in connection with the abuse of a position of trust analysis, the relevant sentencing guideline contemplates the classification level of the information at issue, but it does not address the quantity of materials, nor the number of impacted agencies, nor the length of time the scheme continued, nor even whether the information was transmitted or merely retained—all of which are plainly relevant for purposes of the 3553(a) factors in this case. *See Ford*, 288 F. App'x at 61 (finding no abuse of discretion in district court's departure downward from a guideline range of 108-135 months to a sentence of 72 months because the Top Secret information in that case was retained rather than transmitted). Looking at these factors, they clearly counsel for a significant sentence. The offenses of conviction reflect a pattern of conduct by the defendant over the span of well over a year. This was not one regrettable occurrence, nor was it a fit of piqued conscience. To the contrary, it was a well-thought out scheme to retain and disclose classified national defense information; one that the defendant enhanced over time to minimize the risk of detection. The facts described above chronicle the detailed and calculated steps the defendant took to conceal his actions over time: from arriving early at work on the days that he intended to photograph documents (ostensibly to arrive before his colleagues in order to avoid detection); to manipulating photographed documents into new file formats to better conceal their origin and deleting the materials he had transferred to his laptop; to downloading encrypted email programs; to wiping his laptop after the initial communication of

materials to Reporter A. Further, the defendant exploited the training he received and the information he learned in connection with his job in facilitating the offense. The extent of the defendant's scheme must be reflected in the sentence.

B. History and Characteristics of Defendant

The defendant was born in Santa Rosa, CA, in 1979. The PSR indicates that the defendant had a somewhat difficult upbringing (PSR ¶¶ 39-45), but that did not prevent the defendant from graduating from college and fashioning a reasonably successful 18-year career in the FBI. Defendant chose to move to Minnesota, the childhood home of his wife, in 2012. (PSR ¶ 46). Despite his stated concerns about bias, defendant never sought a transfer to another FBI office. Nor did he ever file any formal complaints about his treatment, the treatment of others, or any particular policies and practices of the FBI.

C. The Need for the Sentence to Afford Adequate Deterrence to Criminal Conduct, and the Need for the Sentence Imposed To Protect the Public from Future Crimes of this Defendant

Under § 3553(a)(2)(A), the court is required to consider “the need to reflect the seriousness of the offense and to promote respect for the law.” As described above, the offenses of conviction are grievous.

General deterrence is the public response necessary to deter other people from committing similar crimes. “Congress specifically made general deterrence an appropriate consideration . . . and we have described it as ‘one of the key purposes of sentencing.’” *Ferguson v. United States*, 623 F.3d 627, 632 (8th Cir. 2010) (quoting *United States v. Medearis*, 451 F.3d 918, 920 (8th Cir. 2006)). A significant sentence of incarceration is appropriate because individuals similarly situated to the defendant need to know that anyone who breaks his or her oath to protect classified information will be punished accordingly. Such a sentence will

deter others who are entrusted with our country's sensitive national security information and would consider compromising it. Accordingly, a custodial sentence at the midpoint of the guideline range will promote respect for the law and afford adequate deterrence to similar criminal conduct in the future. In light of the defendant's actions and his clear disrespect for the law and his profession, as well as his continued knowledge of classified national defense information, a guideline sentence would communicate that the defendant's crimes will not be tolerated and would deter future crimes.

D. The Kinds of Sentences Available, the Need to Avoid Disparities, and the Sentencing Guidelines and Related Policy Statements

Admittedly, it is difficult to compare sentences in cases where classified information is disclosed. The cases vary greatly in the nature of the information at risk from the perspective of the Government. The United States must balance the need for prosecution with the damage that further disclosure of classified information at trial might cause in each instance. Thus, the government often resolves the matters through a specifically negotiated 11(c)(1)(C) plea because the underlying classified equities counsel in favor of such a resolution. *See, e.g., United States v. Winner*, (S.D. Ga. 1:17-cr-00034-JRH-BKE) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, to 63 months for unlawful disclosure of national defense information classified at the Top Secret level); *United States v. Sachtleben*, (S.D. Ind. 1:13-cr-00200-WTL) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, to 43 months for unlawful disclosure of national defense information classified at the Secret level); *United States v. Kiriakou*, (E.D. Va. 1:12-cr-00127-LMB) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, to 30 months for disclosing information identifying CIA officers, including one who was covert); *United States v. Kim*, (D.D.C. 1:10-cr-00225-CKK) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, to 13 months for providing a reporter the contents of a Top Secret//SCI intelligence report); *United*

States v. Leibowitz, (D. Md. 8:09-cr-00632-AW) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, to 20 months for unlawful transmission of five documents classified at the Secret level); *cf. United States v. Sterling*, (E.D. Va. 1:10-cr-00485-LMB) (defendant sentenced, following trial, to 42 months for providing Top Secret classified information published in a book). It is difficult to make comparisons to these other cases involving unauthorized disclosures of classified information to the media, as the challenges related to that information are unique to each case. Each of these cases presents a different tension between the prosecutorial and intelligence interests at stake. Further, when such cases are resolved through guilty pleas, many of the facts underlying those pleas remain classified. Thus, making comparisons between cases based on publicly available information is of little utility. Of note, however, is that the volume of classified information involved in the present case is far greater than any of the aforementioned cases.

Further, there are few prosecutions that closely approximate this one, given the duration of the defendant's activities in collecting and doling out Government secrets. *Cf. Morison*, 844 F.2d 1057 (defendant sentenced to 24 months for disclosure of several documents containing national defense information classified at the Secret level). Moreover, sentences in retention cases also vary, but bear mention. *Compare United States v. Pho*, 1:17-cr-00631 (D. Md. 2018) (sentence of 66 months for unlawful retention of materials classified as Top Secret); *Ford*, 288 F. App'x at 61 (affirming 72 month sentence for retention of materials classified as Top Secret) and *United States v. Marshall* (S.D. TX 1: 17-cr-1) (sentence of 41 months for unlawful retention of materials classified at the Secret level) *with United States v. Mehalba*, 03-cr-10343-DPW (D. Ma. 2005) (20 month sentence in connection with plea for unlawful retention in violation of 793(e) and two counts of violating 18 U.S.C. 1001; court departed downward due to mental

health of defendant). The retention crime here was essentially in service to the defendant's continuing course of conduct in connection with the defendant's transmission of classified materials, and the sentence should reflect that exacerbating fact.

Based on this record, the Government believes a sentence at the midpoint of the guideline range (approximately 52 months) is sufficient, but not greater than necessary, to satisfy the sentencing factors described in 18 U.S.C. § 3553(a).

Dated: October 4, 2018

Respectfully Submitted,

JOHN C. DEMERS
Assistant Attorney General
for National Security
Attorney for the United States,
Acting Under Authority Conferred
by 28 U.S.C. § 515

JEFFERSON B. SESSIONS III
United States Attorney General

G. ZACHARY TERWILLIGER
United States Attorney for
The Eastern District of Virginia

By: S/Patrick T. Murphy
S/David C. Recker
Patrick T. Murphy
Bar No. 2750602 (NY)
David C. Recker
Bar No.0281189 (MN)
Trial Attorneys
National Security Division
950 Pennsylvania Ave. NW
Washington, DC 20530
Patrick.Murphy@usdoj.gov
David.Recker@usdoj.gov
(202) 233-0986

S/ Danya E. Atiyeh
Danya E. Atiyeh
Bar No. 81821 (VA)
Assistant United States Attorney
Special Assistant to the Attorney General
Eastern District of Virginia
2100 Jamieson Ave.
Alexandria, VA 22314
Danya.Atiyeh@usdoj.gov
(703) 299-3700